Lecture 6: Cosets and the Theorem of Lagrange

Prof. Dr. Ali Bülent EKİN
Doç. Dr. Elif TAN

Ankara University

Cosets

Let $(G, \cdot)$ be a group and $H \leq G$. We give two partitions of G by defining the following equivalence relations. Here G may be finite or infinite order.

- Let define the relation $\sim_L$ on G by $a \sim_L b \Leftrightarrow a^{-1}b \in H$. Then $\sim_L$is an equivalence relation on G.
- Similarly, the relation $\sim_R$on G defined by $a \sim_R b \Leftrightarrow ab^{-1} \in H$ is an equivalence relation on G.

The equivalence relation $\sim_L$defines a partition on G. For $a \in G$,

$$\begin{aligned} \bar{a} &= \{x \in G \mid a \sim_L x\} \\ &= \left\{x \in G \mid a^{-1}x \in H\right\} \\ &= \left\{x \in G \mid a^{-1}x = h; \exists h \in H\right\} \\ &= \{ah \mid h \in H\} \\ &= aH. \end{aligned}$$

Similarly,

$$Ha = \{ha \mid h \in H\}.$$

Cosets

Definition

Let $(G, \cdot)$ be a group and $H \leq G$.

- The subset $aH = \{ah \mid h \in H\}$ of G is called the **left coset** of H in G (containing a).
- The subset $Ha = \{ha \mid h \in H\}$ of G is called the **right coset** of H in G.

Remark:

- If G is an abelian group, then $aH = Ha$.
- $eH = H$
- The partition of $\mathbb{Z}$ into cosets of $n\mathbb{Z}$ is equal to the partition of $\mathbb{Z}$ into residue classes modulo n.

Examples:

1. The cosets of $3\mathbb{Z}$ are

$$\begin{aligned} 3\mathbb{Z} &= \{\ldots,-3,0,3,\ldots\} \\ 1+3\mathbb{Z} &= \{\ldots,-2,1,4,\ldots\} \\ 2+3\mathbb{Z} &= \{\ldots,-1,2,5,\ldots\}. \end{aligned}$$

Thus

$$3\mathbb{Z} \cup 1+3\mathbb{Z} \cup 2+3\mathbb{Z} = \mathbb{Z}.$$

Since $\mathbb{Z}$ is abelian the left coset is also a right coset.

2. The partition of $\mathbb{Z}_6$into cosets of the subgroup $H = \{\overline{0}, \overline{3}\}$ are

$$\begin{aligned} H &= \{\overline{0}, \overline{3}\} \\ 1 + H &= \{\overline{1}, \overline{4}\} \\ 2 + H &= \{\overline{2}, \overline{5}\}. \end{aligned}$$

Thus

$$H \cup 1 + H \cup 2 + H = \mathbb{Z}_6.$$

The Lagrange's Theorem

Now we give some important theorems which allows us to prove the Lagrange's Theorem.

Theorem

Let $(G, \cdot)$ be a group and $H \leq G$. For $a, b \in G$,

$$\begin{aligned} (i)\ aH &= bH \Leftrightarrow b^{-1}a \in H \\ (ii)\ Ha &= Hb \Leftrightarrow ab^{-1} \in H \\ (iii)\ aH &= H \Leftrightarrow a \in H. \end{aligned}$$

Theorem

Let $(G, \cdot)$ be a group and $H \leq G$. Then the elements of H are in one-to-one correspondence with the elements of any left (right) coset of H in G.

That is, the function $f : \underset{h \to}{H \to} \underset{ah}{aH}$ is $1-1$ and onto. Thus $|H| = |aH| = |Ha|$.

The Lagrange's Theorem

Theorem

Let $(G, \cdot)$ be a group and $H \leq G$. Then there is a one-to-one correspondence of the set of left cosets of H in G onto the set of right cosets of H in G.

That is, let $L := \{aH \mid a \in G\}$ and $R := \{Ha \mid a \in G\}$ be the sets of all left and right cosets of H in G, respectively. Then

$$f : \begin{array}{ccc} L & \to & R \\ aH & \to & Ha^{-1} \end{array}$$

is $1-1$ and onto. Thus there are the same number of left cosets as the right cosets.

Index

Definition

Let $(G, \cdot)$ be a group and $H \leq G$. Then the number of distinct left (right) cosets, written $[G : H]$, of H in G is called the **index** of H in G.

- If G is finite $\Rightarrow [G : H]$ is finite.
- If G is infinite $\Rightarrow [G : H]$ may be finite or infinite.

Examples:

1. $[\mathbb{Z} : n\mathbb{Z}] = n$
2. $[\mathbb{Q} : \mathbb{Z}] = \infty$

Theorem (The Lagrange's Theorem)

Let H be a subgroup of a **finite** *group G. Then $|H| \mid |G|$.*

Proof of Synopsis:

- Since G is finite, the number of left cosets of H in G is finite.
- G is disjoint union of left cosets of H
- Each left cosets has as many elements as H
- This gives

$$|G| = [G : H].|H|$$

which implies $|H| \mid |G|$.

Corollary

1. *Every group of prime order is cyclic.*
2. *Let* $(G, \cdot)$ *be a group of order* n. *Then for* $a \in G$, $\circ(a) \mid n$ *and* $a^n = e$.
3. *Let* H *and* K *be finite subgroups of a group* G. *Then*

$$|HK| = \frac{|H|\,|K|}{|H \cap K|}.$$

Remark: A natural question can be asked as "The converse of Lagrange's theorem is true?" That is, if G is a group of order n, and $m \mid n$, then is there any subgroup of order m?

- From now on, we know that it is true for finite cyclic groups .
- Later we will see that it is true for abelian groups. But we will give a contrary example for nonabelian groups. In particular, the alterne group A_4 $(|A_4| = 12)$ has no subgroup of order 6, although $6 \mid |A_4|$.